Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
1		**General – IA Policy and Guidance**			
1a	DODI 5000.02 DAG	• Define the full-spectrum IA and CND process from requirements (technical and operational), to systems engineering, C&A, DIACAP, ATO, DT and OT to avoid confusion with PMs and PEOs. • Details of the process should be added to the DOD Acquisition Guidebook (DAG) to provide over-arching, and definitive guidance when questions arise.	Section 2.1.1 bullet 1	AT&L	ASD(NII)/DoD CIO DOT&E
1b	DODI 5000.02	Reference and mandate DOT&E IA guidance, which articulates system requirements to the system acquisition process, but is mostly unknown to the acquisition PM.	Section 2.1.1 bullet 2	AT&L	DOT&E
1c	DODI 5000.02	Insert relevant sections of updated DOT&E Guidance - *Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Program*s and CND that pertain to increasing acquisition oversight and enforcement of IA and CND T&E activities.	Section 2.1.1 bullet 3	AT&L	DOT&E
1d	DODI 5000.02	Modify to include, for each applicable acquisition milestone, the entrance and exit criteria associated with planning and executing IA T&E and C&A.	Section 2.1.1 bullet 4	AT&L	DOT&E ASD(NII)/DoD CIO
1e	CJCSI 3170 JCIDS documents	• The NSS as defined by the DODD/I 8500 Information Assurance series should include identification of the Tier III and Tier II CNDSPs as defined in the DODD 8530 CND. This would enable the MAC and CL assignments, and the CNDSP, if known, to be identified as part of the capabilities based assessment and to be documented in the Initial Capabilities Document (ICD) produced for the DODI 5000.02 MDD. • If the CNDSP is not known Pre-MDD, a requirement should be established for validation of the CNDSP as entrance criteria for the Technology Development phase to ensure that the information is obtained prior to MS-B and incorporated in the Capability Development Document (CDD).	Section 2.1.1 bullet 5	CJCS	ASD(NII)/DoD CIO AT&L
1f	CJCSI 6212	Document should be changed to require that the MAC and CL assignments, and the Tier II and III CNDSPs be documented in the ICD, CDD and CPD.	Section 2.1.1 bullet 6	CJCS	ASD(NII)/DoD CIO AT&L
1g	CJCSI 6212 DODD/I 4630	Add a requirement stating that operational and systems interfaces with Tier II and III CNDSPs are to be documented in the appropriate architectural views.	Section 2.1.1 bullet 7	CJCS ASD(NII)/DoD CIO	AT&L

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
1h	DODD 8530.1	CND policy should mandate periodic performance based measurement of Tier II and III CND protect, detect, react, and restore measures to document the performance basis of the underlying infrastructure.	Section 2.1.1 bullet 8	ASD(NII)/DoD CIO	US STRATCOM
2		**General – Workforce**			
2a	DOD IA curricula	• Identify gaps in IA training needed to prepare systems engineering and program management professionals for effectively participating in all phases of the systems acquisition process. • Emphasize IA skills required to successfully participate in the early phases of systems acquisition such as IA systems engineering, IA Integrated Product Team (IPT), Integrated Test Team (ITT), and as IA and CND penetration/exploitation testers. • Emphasize assurance disciplines, such as IA risk and threat analysis, software assurance, and Supply Chain Risk Management (SCRM).	Section 2.1.2 bullet 1	AT&L	ASD(NII)/DoD CIO DOT&E
2b	DAU	• Training and certification should be added for acquisition professionals where required to address the gaps. • IA training should comprehensively address the critical IA knowledge needed for acquisition program testing.	Section 2.1.2 bullet 1	AT&L	DOT&E NSA ASD(NII)/DoD CIO
2c	Systems Engineering curricula	• Training and certification should be added to systems engineering curricula where required to address the gaps. • IA training should comprehensively address the critical IA knowledge needed for acquisition program testing.	Section 2.1.2 bullet 1	AT&L	DOT&E
2d	Practice	The IA acquisition and T&E teams should supplement in-house knowledge and experience by recruiting IA personnel from industry and academia with ethical hacking skills that can recreate malicious attacks from the attackers' viewpoint.	Section 2.1.2 bullet 2	AT&L	DOT&E
2d	DAU & DOD IA curricula	Once the proposed accelerated IT acquisition process is developed, training courses should be enhanced and additional courses developed if necessary to support IA activities in the new process.	Section 2.1.2 bullet 3	AT&L	DOT&E
3		**Requirements Definition, Systems Engineering and Process Execution**			

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
3a	DODI 5000.02 Practice	An ITT should be established as early as possible in the acquisition process, and should consist of representatives from the developmental, operational, security, and interoperability T&E communities. The collaboration of the ITT members is critical to achieving the vision of "test by one, accept by many."	Section 2.2.1 bullet 1	AT&L	DOT&E
3b	Practice IA/CND T&E guidance	The ITT should collaborate with the acquisition and engineering communities to ensure that meaningful, measurable T&E criteria are identified to evaluate IA capabilities.	Section 2.2.1 bullet 2	AT&L DOT&E & AT&L	ASD(NII)/DoD CIO
3c	DAG	The ITT should be an active participant in the systems engineering process and participate in program and technical reviews.	Section 2.2.1 bullet 3	AT&L	DOT&E ASD(NII)/DoD CIO
3d	Practice IA/CND T&E guidance	• The ITT should convene with the development team to strategize on an integrated DT and OT T&E plan. • IA and CND T&E criteria should not only establish minimum technical thresholds, but also address the operational criteria suggested in the DOT&E Six-Step process.	Section 2.2.1 bullet 4	AT&L DOT&E & AT&L	DOT&E ASD(NII)/DoD CIO
3e	Practice DODI 5000.02 JCIDS documents	IA capabilities and requirements should be addressed in the early Systems Engineering Technical Reviews (SETRs) and translated into robust system requirements, RFPs, and the IT system preliminary design. Translating IA requirements into system requirements and specifications early on will ensure more positive T&E outcomes during later acquisition test phases.	Section 2.2.1 bullet 5	AT&L CJCS	ASD(NII)/DoD CIO DOT&E
3f	IA/CND T&E guidance	• IA T&E criteria should include minimum technical thresholds such as Measures of Performance (MOP), and Measures of Effectiveness (MOE) that address the operational criteria as suggested in the DOT&E Six-Step process in order to evaluate end-to-end IA capabilities. • Technical and operational thresholds should be used to evaluate significant IA controls and concerns, including the ability to protect, detect, react and restore systems to sustain continuity of operations.	Section 2.2.1 bullet 6	AT&L & DOT&E	ASD(NII)/DoD CIO

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
3g	Practice IA/CND T&E guidance	IA T&E should be conducted during Step 4 of the DOT&E IA OT process concurrent with DT using operationally realistic testing environments and representative threats. Step 4 IA T&E should not be confused with penetration testing using Red Teams that is usually performed in step 5 and is only applied to the SUT.	Section 2.2.1 bullet 7	AT&L DOT&E & AT&L	ASD(NII)/DoD CIO
3h	Practice JCIDS documents	• An IA IPT that is comprised of all IA stakeholders should be formed and include representatives from DT&E, C&A, OT&E IA and CND testers, PM, system developer, and representatives of the intended CNDSP and local enclaves that will provide the inherited CND protection for the system being acquired. • The IA IPT should form prior to Milestone B. IA IPT formation guidance should be added to JCIDS documents.	Section 2.2.2 bullet 1	AT&L CJCS	DOT&E AT&L
3i	DAG IA/CND T&E guidance	The IA IPT should work in close coordination with the ITT and engage in all phases of acquisition and engineering to confirm that appropriate technical and operational IA requirements have been established and that T&E activities will identify IA issues at the earliest possible opportunity.	Section 2.2.2 bullet 2	AT&L DOT&E & AT&L	 ASD(NII)/DoD CIO
3j	DODI 5000.02	Program Protection planning and IA must be addressed in the early phases of systems acquisition and systems engineering.	Section 2.2.2 bullet 3	AT&L	ASD(NII)/DoD CIO
3k	JCIDS documents	Capabilities documents should contain sufficient detail to derive both operational and technical IA requirements.	Section 2.2.2 bullet 4	CJCS	AT&L ASD(NII)/DoD CIO DOT&E
3l	CJCSI 6212	MAC and CL should be explicitly stated in the capabilities documents, specifically the ICD, CDD and CPD.9	Section 2.2.2 bullet 5	CJCS	ASD(NII)/DoD CIO
3m	JCIDS documents	NR-KPP DODAF operational and system viewpoints must depict how IA will be incorporated into the proposed new capabilities.	Section 2.2.2 bullet 6	CJCS	ASD(NII)/DoD CIO
3n	Practice JCIDS documents	Operational IA requirements should be derived from Operating Concepts, CONOPS, and DODAF views, based upon an understanding of the importance of the system's mission execution.	Section 2.2.2 bullet 7	AT&L CJCS	ASD(NII)/DoD CIO

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
3o	JCIDS documents	Capabilities documents should explicitly identify CNDSPs and inherited control domains and sufficient operational detail to derive technical specifications for Net Ready performance characteristics.	Section 2.2.2 bullet 8	CJCS	ASD(NII)/DoD CIO
3p	DODI 5000.02	IA technical and operational requirements should be incorporated into RFPs/contracts and addressed at preliminary and critical design reviews.	Section 2.2.2 bullet 9	AT&L	ASD(NII)/DoD CIO
3q	IA/CND T&E Procedure	Amend guidance to provide recommended mapping of IA controls to PDRR measures. DOT&E should update IA guidance to provide the mappings DOT&E will use when there is a conflict.	Section 2.2.2 bullet 10	DOT&E & AT&L	ASD(NII)/DoD CIO
3r	DODI 5000.02 IA/C&D T&E Procedure	Update guidance to more clearly state under what conditions the OTA can use the C&A Security Test and Evaluation (ST&E) results to meet evaluation requirements and to satisfy the operational IA vulnerability evaluation (Step 4).	Section 2.2.2 bullet 11	AT&L DOT&E & AT&L	ASD(NII)/DoD CIO
3s	DODI 5000.02	All findings and/or status of IA (DT&E, C&A, and OT&E) interoperability certification (CJCSI 6212) and connection approval (CJCSI 6211) processes should be made available to the MDA for MAIS at the Limited Deployment Decision Review (MS-C) and at the Full Deployment Decision Review or for Full Rate Production Decision for a Major Defense Acquisition Program (MDAP).	Section 2.2.2 bullet 12	AT&L	ASD(NII)/DoD CIO DOT&E CJCS
4		**Platform IT**			
4a	DODD 5000.01	Policy should be modified to clarify the need to address PIT IA requirements and subsequent C&A activities.	Section 2.3.1 bullet 1	AT&L	ASD(NII)/DoD CIO
4b	DODD/I 8500 series	Policy should provide additional clarification regarding the policy on PIT, specifically as it relates to non interconnected PIT, to identify the authority responsible for making a determination that an IT component is PIT.	Section 2.3.1 bullet 2	ASD(NII)/DoD CIO	AT&L
4c	DODD/I 8500 series DODD 5000.01	Eliminate the blanket exemption of the DIACAP process for PIT, and instead reinforce DODD 5000.01 by enforcing the establishment of IA requirements for PIT via the MAC and CL assignments, and requiring IA system C&A. In other words, PIT is DIACAP exempt, but not exempt from IA controls or C&A activities.	Section 2.3.1 bullet 3	ASD(NII)/DoD CIO AT&L	AT&L ASD(NII)/DoD CIO

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
4d	Practice DODD/I 8500 series	A process should be created that determines criteria for defining: • Whether MAC and CL assignments are required • IA Controls that should be required, engineered, and applied • Process that should be used for PIT controls to be certified • PIT requirements for Net Ready KPP • Interoperability Test Certification requirements for PIT	Section 2.3.1 bullet 4	AT&L ASD(NII)/DoD CIO	ASD(NII)/DoD CIO AT&L
4e	CJCSI 6212 IA/CND T&E guidance	Modify document to explicitly address PIT and PIT interconnections and how they should be handled by the acquisition and testing communities.	Section 2.3.1 bullet 5	CJCS DOT&E & AT&L	ASD(NII)/DoD CIO
5		**Contracting**			
5a	Practice	Government staff should be augmented with IA SMEs to ensure that appropriate IA requirements and CDRLs are placed on contract. IA SMEs should be involved in RFP development, source selection, contract negotiations and contract monitoring.	Section 2.4.1 bullet 1	AT&L	ASD(NII)/DoD CIO
5b	DODI 5000.02 DAG JCIDS documents	• System specifications, RFPs and contracts should include explicit language addressing both technical and operational IA and systems assurance requirements to include SCRM, software assurance, and IA standards implementation (e.g. FIPS compliance, and Common Criteria). • Measureable and meaningful IA and CND achievements must be attached to each milestone decision point.	Section 2.4.1 bullet 2	AT&L CJCS	ASD(NII)/DoD CIO
5c	DODI 5000.02	The RFP SOW should direct contractors to address IA during PDRs, CDRs, and all technical reviews, and to participate in the ITT.	Section 2.4.1 bullet 3	AT&L	ASD(NII)/DoD CIO DOT&E

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
6		**Realistic IA and CND T&E Environments and Resources**			
6a	DODI 5000.02 DAG IA/CND T&E Procedure	Supplement policy with a set of requirements for a single, joint, and integrated IA and CND T&E methodology.	Section 2.5.1 bullet 1	AT&L DOT&E & AT&L	ASD(NII)/DoD CIO
6b	IA/CND T&E Procedure	The T&E methodology should include clearly enumerated T&E objectives and required data needed to accurately measure and evaluate system IA and CND capabilities. Defining Step 5 OT&E process and procedures is particularly important for realistically portraying the cyber threat.	Section 2.5.1 bullet 1	DOT&E & AT&L	ASD(NII)/DoD CIO NSA/DIA
6c	IA/CND T&E guidance	The Intelligence Community and other responsible organizations must provide the T&E community and supporting activities up-to-date threat characterization information as applicable to all phases of acquisition and T&E.	Section 2.5.1 bullet 2	DOT&E & AT&L	ASD(NII)/DoD CIO NSA/DIA
6d	IA/CND T&E guidance DAG	Develop an interactive process to provide up-to-date threat information to the acquisition and requirements community to include updating the information periodically to ensure currency.	Section 2.5.1 bullet 2	DOT&E & AT&L AT&L	NSA/DIA ASD(NII)/DoD CIO
6e	DOT&E Procedure	The responsible supporting information operations organization should coordinate their threat portrayal with the supporting intelligence community organization and be able to lay out the Tactics, Techniques and Procedures (TTP) and application of that threat to the T&E community and acquisition community.	Section 2.5.1 bullet 2	DOT&E	NSA/DIA ASD(NII)/DoD CIO
6f	JCIDS documents	The requirements community should identify the threat generation environment in which the system is expected to operate (per CJCSI 6510.01E, Generation 1, 2, or 3), which will help determine T&E adequacy.	Section 2.5.1 bullet 2	CJCS	NSA/DIA
6g	DODD 8500.1, DODI 5000.02, DAG	Policy should be modified to recognize acquisition related IA and CND T&E as a critical activity to assure the security of DOD system.	Section 2.5.1 bullet 3	ASD(NII)/DoD CIO AT&L	AT&L ASD(NII)/DoD CIO

Table of Recommended Responsible and Supporting Organizations

Item	Policy/ Guidance	IA Cross Walk Working Group Recommendations	Document Reference	Responsible Organization	Supporting Organization(s)
6h	IA/C&D T&E guidance	• Designated information operations, intelligence, emerging cyber and other organizations with the responsibility of providing penetration and exploitation testing supporting acquisition T&E requirements, should provide sufficient, timely services that portray operationally realistic threats and employ techniques that will satisfy test adequacy requirements during IA and CND acquisition test events. • Services and Components should examine their processes and capacity for providing penetration and exploitation testing in support of acquisition IA and CND requirements. If the examination finds existing means for providing penetration and exploitation testing to address IA and CND T&E requirements are not adequate, then the Services and Components should consider establishing penetration and exploitation testing capabilities dedicated to supporting the acquisition T&E community.	Section 2.5.1 bullet 4	DOT&E & AT&L DOT&E & AT&L	ASD(NII)/DoD CIO NSA/DIA ASD(NII)/DoD CIO NSA/DIA
6i	IA/CND T&E guidance DAG	The acquisition T&E community should ensure that the testing associated with Step 5 of the DOT&E Six-Step process is performed in the operational environment in which the SUT will reside after fielding. If the operational environment cannot be used, then a simulated realistic environment should be used. This environment should be proposed in the TES and TEMP and, if appropriate, approved by OSD.	Section 2.5.1 bullet 5	DOT&E &AT&L AT&L	ASD(NII)/DoD CIO